Software Supply Chains

Robert J. Ellison, Christopher Alberts, Rita Creel, Audrey Dorofee, and Carol Woody

The SEI Technical Note, Software Supply Chain Risk Management: From Products to Systems of Systems, [1]provides an introduction to software supply chains.

The term “supply chain” has a long history in the business community and includes recent trends such as just-in-time inventory. In the past, the business community considered supply chains as relevant only to the delivery of physical products. Now the business community uses the technology supply chain to develop most IT systems (hardware, software, public and classified networks, and connected devices), which together enable the uninterrupted operations of key government and industrial base actors, such as the Department of Defense, the Department of Homeland Security, and their major suppliers. While we have decades of physical supply chain data that have led to effective management practices, we have limited experience with technology supply chains. Although no optimal solution exists, much can be done to enable organizations to reduce risk effectively and efficiently while leveraging the significant opportunities afforded by supply chains.

On-time delivery and costs often get the most commercial attention, but some of the most serious risks are associated with system assurance, the confidence that the system behaves as expected. Software defects, such as design and implementation errors, can lead to unexpected behaviors or to system failure. Defects that enable an attacker to purposely change system behavior are often referred to as vulnerabilities. The source of such vulnerabilities is the technology supply chain, which includes commercial product vendors, custom development and integration contractors, and suppliers and subcontractors to those organizations.

Supply chain analysis cannot be limited to those of the most critical products as cyber attacks seek weak points anywhere in the chain but not necessarily weak points in the target. A good example is the Stuxnet malware which is discussed in the report. The attack objective appeared to be to compromise specific control systems, but those systems were not compromised directly. Instead, the malware was designed to infect hundreds of thousands of computers which hopefully would include a few that were used by system administrators for targeted control systems.

The SEI technical note considers supply chains for products, systems and systems of systems. Most attacks initially exploit defects in a system component which is frequently a commercial product. System integration may have to mitigate the supply chain risks associated with using a component. The Stuxnet example is more of a system of systems issue. The implicit trust that often exists between internal systems in an organization can be exploited.

SEI Supply Chain Reports

· Evaluating and mitigating software supply chain security risks[2]

· Software Supply Chain Risk Management: From Products to Systems of Systems[3]

Related supply articles on Build-Security-In

· A systemic approach for assessing software supply-chain risk[4]

· Supply-chain risk management: Incorporating security into software development[5]

1. http://www.sei.cmu.edu/library/abstracts/reports/10tn026.cfm
2. http://www.sei.cmu.edu/library/abstracts/reports/10tn016.cfm
3. http://www.sei.cmu.edu/library/abstracts/reports/10tn026.cfm
4. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/acquisition/1230-BSI.html (A Systemic Approach for Assessing Software Supply-Chain Risk)
5. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/acquisition/1140-BSI/version/live (Supply-Chain Risk Management: Incorporating Security into Software Development)

· Improving Software Assurance and Top 25 CWE Lists[6]

· Considering software supply-chain risk[7]s

6. http://buildsecurityin.us-cert.gov/bsi/resources/articles/1122-BSI/version/live (Improving Software Assurance and Top 25 CWE Lists)
7. http://buildsecurityin.us-cert.gov/bsi/resources/1185-BSI/1207-BSI/version/live (Considering Software Supply Chain Risks©)